REMARKS

Claims 23 - 50 remain pending in the present application. The rejections set forth in the Office Action are respectfully traversed below.

Rejections Under 35 U.S.C. §112, Second Paragraph:

Claims 23 - 50 were rejected under 35 U.S.C. §112, second paragraph. Independent claim 23 was amended to clarify features of the present invention. The six items identified in the Office Action with regard to claim 23 are rendered moot by amended claim 23. Therefore, independent claim 23 meets all the requirements under 35 U.S.C. §112, second paragraph, and the rejection thereof should be withdrawn.

The rejections of claims 24 - 29 should be withdrawn since these claims were only rejected under §112, second paragraph because of the rejection of base claim 23.

The rejection of claim 30 should be withdrawn since the Office Action incorrectly alleges that claim 30 is a duplicate of claim 29. A careful reading of claims 29 and 30 will reveal that claim 21 recites that the encrypted digital data is decrypted to decrypted digital data "**only when**" the digital data is displayed or edited. This exclusivity is not repeated in claim 30.

The rejections of claims 31 - 40 withdrawn since base claim 23 meets all the requirements under §112, second paragraph.

The rejections of claims 41 - 46 should be withdrawn since the claimed subject matter is definite. The Office Action rejected these claims, questioning the ***purpose*** for various claimed

D

features in these claims. However, the applicant is not required to recite the purpose for claimed limitations.

The rejections of claims 47 and 48 should be withdrawn since there base claims meet all the requirements under §112, second paragraph.

Claims 49 and 50 were amended to reword the claimed subject matter to clarify features of the present invention. For instance, that which is encrypted again is the part of the digital data, excluding the copyright information. The copyright information portion of the digital data is not encrypted again along with the rest of the digital data. Moreover, it should be noted that claim 50 does not depend from claim 48 as alleged at the bottom of page 4 of the Office Action. Amended claims 49 and 50 meet all the requirements under §112, second paragraph.

<u>Rejections Under 35 U.S.C. §103</u>:

Claims 23 - 50 were rejected under 35 U.S.C. §103 over **Lee et al.** (USP 5,606,613), in view of **Lynn et al.** (USP 5,345,508), **Smid et al.** (USP 4,386,233), **Bartoli et al.** (USP 5,353,351), and **Eyer et al.** (USP 5,485,577).

First, these prior art rejections should be withdrawn since they rely on the primary reference to **Lee** which is not prior art. **Lee** was issued on February 25, 1997, from an application filed on December 22, 1994. Pursuant to 35 U.S.C. §119, the Applicant is entitled to the benefit of its foreign priority application date of April 1, 1994 which antedates the filing date of **Lee**, thereby removing **Lee** as "prior art." For at least this reason, the §103 rejections should be withdrawn.

D

Nevertheless, nothing in the references to **Lee**, **Lynn**, **Smid**, **Bartoli**, and **Eyer**, either alone or in combination, discloses all the features recited in the present claimed invention. One fundamental error in the prior art rejections was the reliance on general concepts of decryption and encryption using a cryptographic key (such as by the references to **Lee**, **Lynn**, **Smid**, and **Bartoli)** for allegedly disclosing the present claimed use of a utilization permit key. The present claimed invention recites a specific correspondence between a utilization permit key and at least one of several different operations that may be performed on digital data. Decryption of encrypted data relies on the use of the correct utilization permit key. For instance, data encrypted using an edit permit key cannot be decrypted using a storage permit key. The cited art does not disclose or suggest any pre-defined correlation between any utilization permit key and specific types of operations or actions that may be performed on digital data.

As stated in the Office Action, the prior art merely encrypts and decrypts. Once ciphertext is decrypted into plain text, any arbitrary operation or action may be performed on the plain text (*see e.g.*, page 10 of the Office Action). The cited art does not teach or suggest the present claimed invention which requires decryption using an appropriate utilization permit key in order to perform the desired operation on a digital data (*e.g.*, display, edit, copy, store, or transfer) specifically associated with the particular utilization permit key. For at least these reasons, the present invention patentably distinguishes over the prior art.

The dependent claims recite further features not taught or suggested in the prior art. For instance, some dependent claims further recite using a copyright management program, adding copyright information, or a hierarchy for the various utilization permit keys. It should be noted that the prior does not even address copyrights or copyright information. Under U.S. Copyright law, copyrights include identification of authorship, title, date of creation, and publication of the work. The prior art is only directed to simple encryption and decryption, without any concern as to any copyrights of the data encrypted or decrypted, nor the control and management of any copyrights of the digital data involved - and not through the use of a copyright management program or copyright information. For at least these reasons, the dependent claims further distinguish over the cited prior art.

The Office Action referred to **Eyer** for allegedly obviating the present claimed hierarchy for the utilization permit keys. However, the "key hierarchy" according to **Eyer** is directed to different authorization levels for accessing encrypted data. Such "key hierarchy" for access levels is different from the present claimed hierarchy for utilization permit keys permitting selected operations on digital data. As mentioned above, the present claimed utilization permit keys permits at least one of displaying, editing, storing, copying, and transferring of digital data. Certain operations are only permitted with certain utilization permit keys. For instance, encrypted digital data cannot be decrypted with a *storage* permit key for *editing* of digital data. Such specific control over specified actions on the digital data is not taught or suggested in the cited prior art (neither in **Eyer** nor in the other cited references). Moreover, the added limitation for a hierarchy for the utilization permit keys, for example, an edit permit key being at the highest level in the hierarchy (thereby permitting all of the other operations at lower levels in the hierarchy), is not taught or suggested in the prior art. Such claimed correspondence between utilization permit keys and specific operations (and a hierarchy for such keys, controlling operations at lower hierarchy levels) patentably distinguishes over the prior art.

It should also be noted that the Office Action relies on no less than five (5) different art references in order to substantiate its rejections under 35 U.S.C. §103. The motivation to combine each and every one of these cited reference with each and other one of the other references has not been provided. Pursuant to MPEP §2143.01, the burden is upon the Examiner to set forth the basis for the suggestion or motivation to modify the references in the manner claimed, in the first instance. The mere fact that references "can" be combined and/or modified does not render the resulting combination obvious unless the prior art also suggest the desirability of the combination. Without identifying the requisite motivation to combine in the manner claimed, the Examiner has not provided the Applicant with a basis to question whether any particular reference *teaches away* from the asserted combination(s), whether *undue experimentation* is required to modify a reference, or whether the asserted combination would *defeat the primary purpose* of any particular reference. For at least these further reasons, the rejections under §103 should be withdrawn since a *prima facie* case of obviousness has not been established.

Summary:

For the detailed reasons set forth above, the present claimed invention patentably distinguishes over the prior art. The amended claims also clarify features of the claimed invention, thus rendering moot the rejections under 35 U.S.C. §112, second paragraph. Therefore, the pending claims are now in condition for allowance and a Notice of Allowance is respectfully requested.

D

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "**Version with markings to show changes made**."

In the event that this paper is not timely filed, Applicant respectfully petitions for an appropriate extension of time. Please charge any fees for such an extension of time and any other fees which may be due with respect to this paper, to Deposit Account No. 01-2340.

Respectfully submitted,

ARMSTRONG, WESTERMAN & HATTORI, LLP

John P. Kong
Attorney for Applicant
Reg. No. 40,054

JPK/kal
Atty. Docket No. **990812A**
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
(202) 659-2930

23850
PATENT TRADEMARK OFFICE

Enclosures: Version with markings to show changes made
H:\HOME\JPK\Mitsubishi\990812a\Filings\Amendment

D

VERSION WITH MARKINGS TO SHOW CHANGES MADE 09/544,497

IN THE SPECIFICATION:

The paragraph beginning on page 15, line 30 through page 16, line 4 has been replaced with the following rewritten paragraph:

Among these methods [for], the method that integrates the copyright information with file header, if the data is character information [is] expressed with character code, [it] is available even without a file header. Thus, the method is simple, but not very reliable. Also, because the capacity of the file header is not high, it is not sufficient if there is a large amount of copyright information.

IN THE CLAIMS:

Claims 23 - 25, 45, 47, 49 and 50 have been amended to read as follows:

23. (Amended) A digital data management method, comprising the steps of:

encrypting digital data to produce encrypted digital data supplied to a user[;], using a utilization permit key [to manage said digital data, said utilization permit key being a display permit key, an edit permit key, a storage permit key, a copy permit key, and/or a transfer permit key;] pre-defined to permit at least one of displaying, editing, storing, copying, and transferring of said digital data;

decrypting said encrypted digital data to decrypted digital data by using [said] a display permit key, which is said utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using [said] an edit permit key, which is said utilization permit key permitting editing of said digital data, and editing said decrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using [said] a storage permit key, which is said utilization permit key permitting storing of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said storage permit key, and storing said encrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using [said] a copy permit key, which is said utilization permit key permitting copying of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said copy permit key, and copying said encrypted digital data; and

decrypting said encrypted digital data to decrypted digital data by using [said] a transfer permit key, which is said utilization permit key permitting transferring of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said transfer permit key, and transferring said encrypted digital data.

24. (Amended) A digital data management method according to claim 23, wherein said [step of encrypting said digital data uses] utilization permit key includes a crypt key specific to said digital data.

D

25. (Amended) A digital data management method according to claim 23, wherein said [step of encrypting said digital data uses] utilization permit key includes a crypt key not specific to said digital data.

45. (Amended) A digital data management method according to claim 41, wherein said copyright information is added in [said] a copyright management program.

47. (Amended) A digital data management method according to claim 41, wherein [said digital data without] said copyright information [cannot be utilized] must be present in order to use said digital data.

49. (Amended) A digital data management method according to claim 47, wherein said digital data [without], excluding said copyright information, is encrypted again to said encrypted digital data by using said utilization permit key.

50. (Amended) A digital data management method according to claim 47, wherein said digital data [without], excluding said copyright information, is encrypted again to said encrypted digital data by a copyright management program.

D